RSA 密码破译报告

冯古豪 2000013175

摘要

在这个项目中，我们实现了多种 RSA 攻击，并最终破解了 16 组 RSA 加密的数据。

1 序言

在这个项目中，我们主要实现的攻击方式主要包括：低加密指数攻击，低加密指数广播攻击，维纳攻击，共模攻击，Copper-Smith 攻击以及基于大整数分解的攻击。其中，我们尝试的大整数分解方式主要包括：费马分解，Pollard-p-1 分解，Pollard-ρ 分解。

2 攻击原理及实验结果

2.1 低加密指数攻击